

LETTER

Quantum Optimal Multiple Assignment Scheme for Realizing General Access Structure of Secret Sharing

Ryutaroh MATSUMOTO[†], Senior Member

SUMMARY The multiple assignment scheme is to assign one or more shares to single participant so that any kind of access structure can be realized by classical secret sharing schemes. We propose its quantum version including *ramp* secret sharing schemes. Then we propose an integer optimization approach to minimize the average share size.

key words: quantum secret sharing, multiple assignment scheme, access structure

1. Introduction

Secret sharing (SS) [1] is a cryptographic scheme to encode a secret to multiple shares being distributed to participants, so that only *qualified* sets of participants can reconstruct the original secret from their shares. Traditionally both secret and shares were classical information (bits). Several authors, e.g. [2]–[4] extended the traditional SS to quantum one so that a quantum secret can be encoded to quantum shares.

A set of participants is called *forbidden* if the set has absolutely no information about the secret. A secret sharing scheme is called *perfect* [5] if every set of participants is always qualified or forbidden. If a set is neither qualified or forbidden in a secret sharing scheme, the scheme is said to be *ramp* or *non-perfect*. A merit of the ramp schemes is to reduce share size (the number of bits or qubits) while keeping the secret size [6]–[8].

Traditionally, the access structure called the threshold structure has been the most focused one, e.g. [1], [2], [7], where a set of participants is qualified if and only if the number of participants is $\geq t$. A scheme with a threshold structure is called a threshold scheme. A well-known method to realize an arbitrary access structure is the multiple assignment scheme proposed by Shamir [1] and named by Ito et al. [9]. On the other hand, Smith [4] showed how to realize an arbitrary access structure in quantum *perfect* secret sharing schemes, while nobody has shown a construction of quantum *ramp* schemes with arbitrary access structures.

The multiple assignment scheme assigns multiple shares of a threshold scheme to single participants, and a single share can be assigned to multiple participants. It is not straight forward to adapt the multiple assignment scheme, as the no-cloning theorem [10] prevents us from making mul-

multiple copies of a single quantum share. The first purpose of this paper is to propose a quantum version of the multiple assignment scheme.

For a given size of secret, it is important to reduce the size of shares. A demerit of multiple assignment scheme in [9] was lack of consideration of share size. Later, Iwamoto et al. [11] proposed an integer optimization approach to minimize the worst-case or the average share size of multiple assignment scheme. The second purpose of this paper is to adapt Iwamoto et al.'s integer optimization problem to our proposed quantum setting.

2. Review of Previous Research Results

By a classical secret sharing scheme, we mean that its secret and its shares are classical information, while by a quantum secret sharing scheme, its secret and its shares are quantum information. For a set T , 2^T denotes its power set $\{T_0 \mid T_0 \text{ is a subset of } T\}$, and we have $|2^T| = 2^{|T|}$.

Firstly, we review the multiple assignment scheme named by Ito et al. [9] and originally proposed by Shamir [1]. The multiple assignment scheme constructs a classical secret sharing scheme with n participants from that with m participants. It is a map Φ from $\{1, \dots, n\}$ to $2^{\{1, \dots, m\}}$. Let W_1, \dots, W_m be the shares of the original secret sharing scheme. The new secret sharing scheme constructed by Φ distributes $\{W_j \mid j \in \Phi(i)\}$ to the i -th participants. For example, suppose that $m = 3$, $n = 2$, $\Phi(1) = \{1, 2\}$, and $\Phi(2) = \{2, 3\}$. Then, in the new constructed secret sharing scheme, the first participant receives $\{W_1, W_2\}$ as his/her share, and the second one receives $\{W_2, W_3\}$ as his/her share. This method works fine with the classical information. But its straightforward extension to the quantum information is *impossible*, because the quantum no-cloning theorem [10] prevents us from distributing the same W_2 to both first and second participants. To avoid this impossibility, we will focus the relation between two shares $\{W_1, W_2\}$ and $\{W_2, W_3\}$, which can be expressed by linear codes, and will propose to transfer the relation to the quantum setting.

A classical secret sharing is said to be linear if any linear combination of shares expresses the corresponding linear combination of secrets [12]. Let \mathbf{F}_q be a finite field with q elements. It was shown that any linear classical secret sharing scheme can be expressed [13, Proposition 1] by a pair of linear codes $C_2 \subset C_1 \subset \mathbf{F}_q^n$ as follows, provided that the linearity is considered over \mathbf{F}_q .

For a classical secret sharing scheme corresponding to

Manuscript received July 1, 2016.

Manuscript revised September 23, 2016.

[†]The author is with the Department of Information and Communications Engineering, Tokyo Institute of Technology, 152-8550 Japan

DOI: 10.1587/transfun.E100.A.726

$C_2 \subset C_1$, the set of secrets is the factor space

$$C_1/C_2 = \{\vec{d} + C_2 \mid \vec{d} \in C_1\}.$$

Therefore a secret $S \in C_1/C_2$ is a subset of C_1 . For a given secret $S \in C_1/C_2$, a vector $X = (X_1, \dots, X_n)$ is chosen uniformly randomly from S . A subset of $\{X_1, \dots, X_n\}$ is distributed to each participant as his/her share. For practical use of secret sharing schemes, it is indispensable to have a criterion by which one can identify qualified or forbidden sets of shares. Let $I \subset \{1, \dots, n\}$, and a set of participants collectively have $\{X_i \mid i \in I\}$ as their shares. Let P_I be the projection map sending $(x_1, \dots, x_n) \in \mathbb{F}_q^n$ to $(x_i)_{i \in I}$, and $P_I(C_1) = \{P_I(\vec{x}) \mid \vec{x} \in C_1\}$. It was shown in [14] that the set of shares expressed by I is qualified iff

$$\dim P_I(C_1) - \dim P_I(C_2) = \dim C_1 - \dim C_2, \quad (1)$$

and is forbidden iff

$$\dim P_I(C_1) - \dim P_I(C_2) = 0. \quad (2)$$

It is known that most of quantum ramp secret sharing schemes can also be described by a pair of linear codes $C_2 \subset C_1 \subset \mathbb{F}_q^n$ as follows [15]. Let $L = \dim C_1 - \dim C_2$, then the dimension of (pure state) quantum secret is q^L and its orthonormal basis can be chosen as $\{|\vec{s}\rangle \mid \vec{s} \in \mathbb{F}_q^L\}$. The linear space of all the possible quantum shares is q^n -dimensional, and its orthonormal basis can be chosen as $\{|\vec{x}\rangle \mid \vec{x} \in \mathbb{F}_q^n\}$. We fix an \mathbb{F}_q -linear map f from \mathbb{F}_q^L to the factor linear space C_1/C_2 , and a quantum secret $|\vec{s}\rangle$ is encoded to

$$\frac{1}{\sqrt{q^L}} \sum_{\vec{x} \in f(\vec{s})} |\vec{x}\rangle, \quad (3)$$

which is the same as the encoding procedure of the CSS quantum error-correcting codes [16], [17]. Equation (3) can be regarded as a quantum state of n particles having dimension q . In this paper *qudit* refers to a quantum object that is represented by q -dimensional complex linear space. Each participant receives a non-overlapping subset of the n particles of Eq. (3) as his/her quantum share.

As well as the classical case, we need a criterion to tell if a set of shares is qualified or forbidden. Recall that a share set is qualified if and only if its complement is forbidden [2], [7] when the quantum secret sharing scheme is a pure-state scheme, which encode a pure-state secret to a pure-state shares [2]. It was also shown [2] that it is sufficient to consider pure-state schemes. Let $I \subset \{1, \dots, n\}$, and a set of participants collectively have I as their shares, that is, the set of participants has the i -th quantum particle among n particles, each of which has dimension q , if and only if $i \in I$. The share set I is qualified if and only if I is qualified and \bar{I} is forbidden in the classical secret sharing scheme constructed from $C_1 \supset C_2$, where $\bar{I} = \{1, \dots, n\}$. In other words, I is qualified if and only if both Eq. (2) with I substituted by \bar{I} and Eq. (1) hold.

3. Proposed Method to Construct a Quantum Ramp Secret Sharing Scheme with a General Access Structure

Suppose that the number of participants is n . Let q be a prime power as before, and the dimension of quantum secret is assumed to be q^L for a positive integer L . Let $\mathcal{A}_Q \subset 2^{\{1, \dots, n\}}$ be the family of qualified sets given as the requirement for a quantum secret sharing scheme to be constructed. Since we have restricted ourselves to the pure-state schemes, the family of forbidden sets must be $\mathcal{A}_F = 2^{\{1, \dots, n\}} \setminus \mathcal{A}_Q$. It is also assumed that \mathcal{A}_Q satisfies the monotonicity condition [5], that is, if $A \in \mathcal{A}_Q$ and $A \subseteq B \in 2^{\{1, \dots, n\}}$ then $B \in \mathcal{A}_Q$. The monotonicity condition of \mathcal{A}_Q implies the monotonicity condition of \mathcal{A}_F in the reverse order, that is, if $B \in \mathcal{A}_F$ and $B \supseteq A \in 2^{\{1, \dots, n\}}$ then $A \in \mathcal{A}_F$.

We introduce some notations from [11]. Let $\vec{y} = (t, x_1, \dots, x_{2^n-1})$. Later t becomes the design parameter of the underlying threshold ramp quantum secret sharing scheme. Specifically, the underlying ramp secret sharing allows reconstruction of the secret only from t or more shares. Let $b(p)_i$ as the i -th bit of the binary representation of a positive integer p . For a set $A \subset \{1, \dots, n\}$, define

$$1(A)_p = \begin{cases} 1 & \text{if there exists } i \in A \text{ with } b(p)_i = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Define 2^n -dimensional vector $a(\ell, A) = (\ell, 1(A)_1, \dots, 1(A)_{2^n-1})$. Let h_p be the number of 1's in the binary representation of a positive integer p , and $\vec{h} = (h_0, h_1, \dots, h_{2^n-1})$. As $\text{IP}_{\vec{p}}^{R2}$ in [11], we solve the following integer optimization problem:

$$\begin{aligned} & \text{minimize} && \langle \vec{h}, \vec{y} \rangle, \\ & \text{subject to} && \langle a(-1, A), \vec{y} \rangle \geq 0, \forall A \in \mathcal{A}_Q, \\ & && \langle -a(-1, A), \vec{y} \rangle \geq L, \forall A \in \mathcal{A}_F, \\ & && \vec{y} \geq 0, \end{aligned}$$

where $\langle \cdot, \cdot \rangle$ denotes the inner product of two vectors. Since the above integer optimization problem is a relaxed version of the original $\text{IP}_{\vec{p}}^{R2}$ in [11], by Theorem 25 of [11] there must be at least one solution \vec{y} to our integer optimization problem. By following [11], one can construct a *classical* ramp secret sharing scheme with n participants, the qualified set \mathcal{A}_Q , the forbidden set \mathcal{A}_F and the classical secret consisting of L symbols in \mathbb{F}_q . Since their construction produces a classical linear secret sharing scheme, it can be described by a nested pair of linear codes $C_2 \subset C_1 \subset \mathbb{F}_q^m$, where $m = x_1 + \dots + x_{2^n-1}$ determined by a solution $\vec{y} = (t, x_1, \dots, x_{2^n-1})$ of the above integer optimization problem. In the construction method [11], (t, L, m) classical ramp secret sharing scheme is the underlying secret sharing scheme used in construction of the desired secret sharing scheme. Observe that the constructed *classical* ramp secret sharing scheme has the minimum average share size, as proved in [11]. Recall that in the constructed classical secret sharing scheme expressed as $C_2 \subset C_1$, a participant receives

some components of $(z_1, \dots, z_m) \in C_1$ as his/her share. Let $V_i = \{j \mid \text{the } i\text{-th share contains } z_j\} \subset \{1, \dots, m\}$.

To avoid violation of the quantum no-cloning theorem, we modify the coding theoretic expression C_1/C_2 and V_i . Note that only expression is modified and the secret sharing scheme itself is not modified. Let $\gamma(j) = |\{i \mid j \in V_i\}|$, and $m' = \gamma(1) + \dots + \gamma(n)$. For $\vec{z} = (z_1, \dots, z_m) \in C_1$, define

$$\phi(\vec{z}) = (\underbrace{z_1, \dots, z_1}_{\gamma(1) \text{ times}}, \dots, \underbrace{z_m, \dots, z_m}_{\gamma(m) \text{ times}}) \in \mathbf{F}_q^{m'}.$$

Let $C'_1 = \phi(C_1)$ and $C'_2 = \phi(C_2)$. Define $V'_i \subset \{1, \dots, m'\}$ such that $\{z_\ell \mid \ell \in V_i\} = \{\phi(\vec{z})_j \mid j \in V'_i\}$ and $V'_i \cap V'_{i'} = \emptyset$ for $i \neq i'$, where $\vec{z} = (z_1, \dots, z_m) \in C_1$. By the disjointedness $V'_i \cap V'_{i'} = \emptyset$ we can avoid the violation of the quantum no-cloning theorem. The above change of notations makes no change in the actual operation of the constructed classical secret sharing scheme. Then the same constructed secret sharing scheme can also be described by the code pair $C'_2 \subset C'_1$. We also have $|V'_1| + |V'_2| + \dots + |V'_n| = m'$.

We construct the ramp quantum secret sharing scheme from $C'_2 \subset C'_1 \subset \mathbf{F}_q^{m'}$ in which the i -th participants receives the j -th qudit among m' qudits if and only if $w_j \in V'_i$, where $(w_1, \dots, w_{m'}) \in C'_1$ and m' qudits are defined from the quantum secret as Eq. (3). Then the constructed quantum secret sharing scheme has \mathcal{A}_Q as its qualified set, \mathcal{A}_F as its forbidden set, and L -qudit in its quantum share, and the average share size is generally small.

Acknowledgment

The author would like to thank Prof. Mitsugu Iwamoto for helpful discussion, and an anonymous reviewer to identify the critical error in the initial manuscript. This research is partly supported by the National Institute of Information and Communications Technology, Japan, and by the Japan Society for the Promotion of Science Grant Nos. 23246071 and 26289116.

References

- [1] A. Shamir, "How to share a secret," *Comm. ACM*, vol.22, no.11, pp.612–613, Nov. 1979. DOI:10.1145/359168.359176
- [2] R. Cleve, D. Gottesman, and H.K. Lo, "How to share a quantum secret," *Phys. Rev. Lett.*, vol.83, no.3, pp.648–651, July 1999. arXiv:quant-ph/9901025, DOI:10.1103/PhysRevLett.83.648
- [3] D. Gottesman, "Theory of quantum secret sharing," *Phys. Rev. A*, vol.61, no.4, March 2000. arXiv:quant-ph/9910067, DOI:10.1103/PhysRevA.61.042311
- [4] A.D. Smith, "Quantum secret sharing for general access structures," Jan. 2000. URL: arXiv:quant-ph/0001087, arXiv:quant-ph/0001087
- [5] D.R. Stinson, *Cryptography Theory and Practice*, 3rd ed., Chapman & Hall/CRC, 2006.
- [6] H. Yamamoto, "Secret sharing system using (k, l, n) threshold scheme," *Electronics and Communications in Japan (Part I: Communications)*, vol.69, no.9, pp.46–54, 1986. (the original Japanese version published in 1985). DOI:10.1002/ecja.4410690906
- [7] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto, "Quantum secret sharing schemes and reversibility of quantum operations," *Phys. Rev. A*, vol.72, no.3, Sept. 2005. arXiv:quant-ph/0505001,

DOI:10.1103/PhysRevA.72.032318

- [8] W. Ogata, K. Kurosawa, and S. Tsujii, "Nonperfect secret sharing schemes," *Advances in Cryptology – AUSCRYPT '92*, Lecture Notes in Computer Science, vol.718, pp.56–66, Springer-Verlag, 1993. DOI:10.1007/3-540-57220-1_52
- [9] M. Ito, A. Saito, and T. Nishizeki, "Multiple assignment scheme for sharing secret," *J. Cryptology*, vol.6, no.1, pp.15–20, March 1993. DOI:10.1007/BF02620229
- [10] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, UK, 2000.
- [11] M. Iwamoto, H. Yamamoto, and H. Ogawa, "Optimal multiple assignments based on integer programming in secret sharing schemes with general access structures," *IEICE Trans. Fundamentals*, vol.E90-A, no.1, pp.101–111, Jan. 2007. DOI:10.1093/ietfsec/e90-a.1.101
- [12] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan, "Secure computation from random error correcting codes," *Advances in Cryptology–EUROCRYPT 2007*, Lecture Notes in Computer Science, vol.4515, pp.291–310, Springer-Verlag, 2007. DOI:10.1007/978-3-540-72540-4_17
- [13] U. Martínez-Peñas, "On the similarities between generalized rank and Hamming weights and their applications to network coding," *IEEE Trans. Inform. Theory*, vol.62, no.7, pp.4091–4095, July 2016. DOI:10.1109/TIT.2016.2570238
- [14] O. Geil, S. Martin, R. Matsumoto, D. Ruano, and Y. Luo, "Relative generalized Hamming weights of one-point algebraic geometric codes," *IEEE Trans. Inform. Theory*, vol.60, no.10, pp.5938–5949, Oct. 2014. DOI:10.1109/TIT.2014.2345375
- [15] R. Matsumoto, "Coding theoretic construction of quantum ramp secret sharing," arXiv:1405.0149, submitted to *J. Cryptology* on December 2014 (manuscript ID JCryptology-D-14-00061).
- [16] A.R. Calderbank and P.W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol.54, no.2, pp.1098–1105, Aug. 1996. arXiv:quant-ph/9512032
- [17] A.M. Steane, "Multiple particle interference and quantum error correction," *Proc. Roy. Soc. London Ser. A*, vol.452, no.1954, pp.2551–2577, 1996. arXiv:quant-ph/9601029